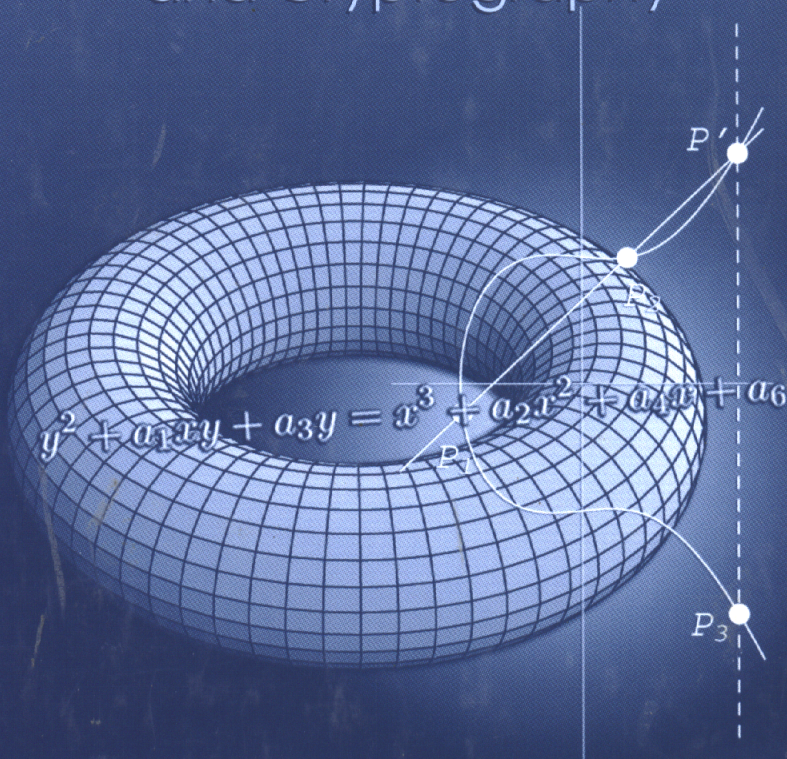


DISCRETE MATHEMATICS AND ITS APPLICATIONS

Series Editor KENNETH H. ROSEN

ELLIPTIC CURVES

Number Theory
and Cryptography



Lawrence C. Washington

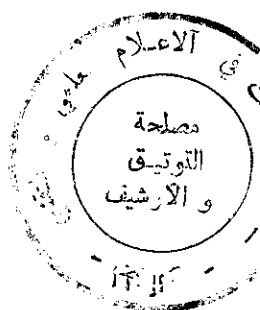


CHAPMAN & HALL/CRC

DISCRETE MATHEMATICS AND ITS APPLICATIONS

Series Editor
Kenneth H. Rosen, Ph.D.

AT&T Laboratories
Middletown, New Jersey



Applications of Abstract Algebra with Maple,
Richard E. Klima, Ernest Stitzinger, and Neil P. Sigmon

Algebraic Number Theory, *Richard A. Mollin*

An Atlas of Smaller Maps in Orientable and Nonorientable Surfaces,
David M. Jackson and Terry I. Visentin

An Introduction to Cryptography, *Richard A. Mollin*

Combinatorial Algorithms: Generation Enumeration and Search,
Donald L. Kreher and Douglas R. Stinson

The CRC Handbook of Combinatorial Designs,
Charles J. Colbourn and Jeffrey H. Dinitz

Cryptography: Theory and Practice, Second Edition, *Douglas R. Stinson*

Design Theory, *Charles C. Lindner and Christopher A. Rodgers*

Enumerative Combinatorics,
Charalambos A. Charalambides

Frames and Resolvable Designs: Uses, Constructions, and Existence,
Steven Furino, Ying Miao, and Jianxing Yin

Fundamental Number Theory with Applications, *Richard A. Mollin*

Graph Theory and Its Applications, *Jonathan Gross and Jay Yellen*

Handbook of Applied Cryptography,
Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone

Handbook of Discrete and Combinatorial Mathematics, *Kenneth H. Rosen*

Handbook of Discrete and Computational Geometry,
Jacob E. Goodman and Joseph O'Rourke

Introduction to Information Theory and Data Compression, Second Edition,
Darrel R. Hankerson, Greg A. Harris, and Peter D. Johnson

Continued Titles

Network Reliability: Experiments with a Symbolic Algebra Environment,
Daryl D. Harms, Miroslav Kraetzl, Charles J. Colbourn, and John S. Devitt

RSA and Public-Key Cryptography
Richard A. Mollin

Quadratics, *Richard A. Mollin*

Verification of Computer Codes in Computational Science and Engineering,
Patrick Knupp and Kambiz Salari

Elliptic Curves: Number Theory and Cryptography
Lawrence C. Washington

DISCRETE MATHEMATICS AND ITS APPLICATIONS

Series Editor KENNETH H. ROSEN

ELLIPTIC CURVES

Number Theory
and Cryptography

Lawrence C. Washington



CHAPMAN & HALL/CRC

A CRC Press Company

Boca Raton London New York Washington, D.C.

BIBLIOTHEQUE DU CERIST

Library of Congress Cataloging-in-Publication Data

Washington, Lawrence C.

Elliptic curves : number theory and cryptography / Lawrence C. Washington.

p. cm. — (Discrete mathematics and its applications)

Includes bibliographical references and index.

ISBN 1-58488-365-0 (alk. paper)

1. Curves, Elliptic. 2. Number theory. 3. Cryptography. I. Title. II. CRC Press series on discrete mathematics and its applications.

QA567.2.E44W37 2003

516.3'52—dc21

2003043972

This book contains information obtained from authentic and highly regarded sources. Reprinted material is quoted with permission, and sources are indicated. A wide variety of references are listed. Reasonable efforts have been made to publish reliable data and information, but the author and the publisher cannot assume responsibility for the validity of all materials or for the consequences of their use.

Neither this book nor any part may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, microfilming, and recording, or by any information storage or retrieval system, without prior permission in writing from the publisher.

The consent of CRC Press LLC does not extend to copying for general distribution, for promotion, for creating new works, or for resale. Specific permission must be obtained in writing from CRC Press LLC for such copying.

Direct all inquiries to CRC Press LLC, 2000 N.W. Corporate Blvd., Boca Raton, Florida 33431.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation, without intent to infringe.

Visit the CRC Press Web site at www.crcpress.com

© 2003 by Chapman & Hall/CRC

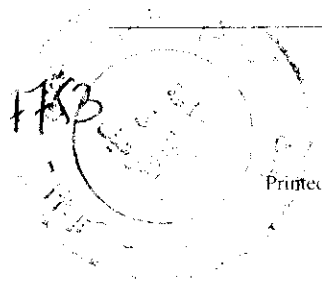
No claim to original U.S. Government works

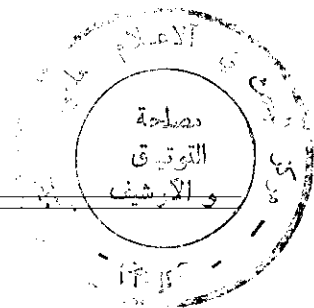
International Standard Book Number 1-58488-365-0

Library of Congress Card Number 2003043972

Printed in the United States of America 2 3 4 5 6 7 8 9 0

Printed on acid-free paper





Preface

Over the last two or three decades, elliptic curves have been playing an increasingly important role both in number theory and in related fields such as cryptography. For example, in the 1980s, elliptic curves started being used in cryptography and elliptic curve techniques were developed for factorization and primality testing. In the 1980s and 1990s, elliptic curves played an important role in the proof of Fermat's Last Theorem. The goal of the present book is to develop the theory of elliptic curves assuming only modest backgrounds in elementary number theory and in groups and fields, approximately what would be covered in a strong undergraduate or beginning graduate abstract algebra course. In particular, we do not assume the reader has seen any algebraic geometry. Except for a few isolated sections, which can be omitted if desired, we do not assume the reader knows Galois theory. We implicitly use Galois theory for finite fields, but in this case everything can be done explicitly in terms of the Frobenius map so the general theory is not needed. The relevant facts are explained in an appendix.

The book provides an introduction to both the cryptographic side and the number theoretic side of elliptic curves. For this reason, we treat elliptic curves over finite fields early in the book, namely in Chapter 4. This immediately leads into the discrete logarithm problem and cryptography in Chapters 5, 6, and 7. The reader only interested in cryptography can subsequently skip to Chapters 10 and 11, where complex multiplication and the Weil and Tate-Lichtenbaum pairings are discussed. But surely anyone who becomes an expert in cryptographic applications will have a little curiosity as to how elliptic curves are used in number theory. Similarly, a non-applications oriented reader could skip Chapters 5, 6, and 7 and jump straight into the number theory in Chapters 8 and beyond. But the cryptographic applications are interesting and provide examples for how the theory can be used.

There are several fine books on elliptic curves already in the literature. This book in no way is intended to replace Silverman's excellent two volumes [90], [92], which are the standard references for the number theoretic aspects of elliptic curves. Instead, the present book covers some of the same material, plus applications to cryptography, from a more elementary viewpoint. It is hoped that readers of this book will subsequently find Silverman's books more accessible and will appreciate their slightly more advanced approach. The books by Knapp [47] and Koblitz [49] should be consulted for an approach to the arithmetic of elliptic curves that is more analytic than either this book or [90]. For the cryptographic aspects of elliptic curves, there is the recent book of Blake et al. [7], which gives more details on several algorithms than the present

book, but contains few proofs. It should be consulted by serious students of elliptic curve cryptography. We hope that the present book provides a good introduction to and explanation of the mathematics used in that book. The books by Enge [28], Koblitz [51], [50], and Menezes [64] also treat elliptic curves from a cryptographic viewpoint and can be profitably consulted.

Notation. The symbols \mathbf{Z} , \mathbf{F}_q , \mathbf{Q} , \mathbf{R} , \mathbf{C} denote the integers, the finite field with q elements, the rationals, the reals, and the complex numbers, respectively. We have used \mathbf{Z}_n (rather than $\mathbf{Z}/n\mathbf{Z}$) to denote the integers mod n . However, when p is a prime and we are working with \mathbf{Z}_p as a field, rather than as a group or ring, we use \mathbf{F}_p in order to remain consistent with the notation \mathbf{F}_q . Note that \mathbf{Z}_p does not denote the p -adic integers. This choice was made for typographic reasons since the integers mod p are used frequently, while a symbol for the p -adic integers is used only in a few examples in Chapter 13 (where we use \mathcal{O}_p). The p -adic rationals are denoted by \mathbf{Q}_p . If K is a field, then \bar{K} denotes an algebraic closure of K . If R is a ring, then R^\times denotes the invertible elements of R . When K is a field, K^\times is therefore the multiplicative group of nonzero elements of K . Throughout the book, the letters K and E are generally used to denote a field and an elliptic curve (except in Chapter 9, where K is used a few times for an elliptic integral).

Acknowledgments. The author thanks Bob Stern of CRC Press for suggesting that this book be written and for his encouragement, and the editorial staff at CRC Press for their help during the preparation of the book. Ed Eikenberg, Jim Owings, Susan Schmoyer, Brian Conrad, and Sam Wagstaff made many suggestions that greatly improved the manuscript. Of course, there is always room for more improvement. Please send suggestions and corrections to the author (lew@math.umd.edu). Corrections will be listed on the web site for the book (www.math.umd.edu/~lew/ellipticcurves.html).

To Susan and Patrick

BIBLIOTHEQUE DU CERIST

Contents

1	Introduction	1
	Exercises	8
2	The Basic Theory	9
2.1	Weierstrass Equations	9
2.2	The Group Law	12
2.3	Projective Space and the Point at Infinity	18
2.4	Proof of Associativity	20
2.4.1	The Theorems of Pappus and Pascal	32
2.5	Other Equations for Elliptic Curves	35
2.5.1	Legendre Equation	35
2.5.2	Cubic Equations	35
2.5.3	Quartic Equations	36
2.5.4	Intersection of Two Quadratic Surfaces	39
2.6	The j -invariant	41
2.7	Elliptic Curves in Characteristic 2	44
2.8	Endomorphisms	46
2.9	Singular Curves	55
2.10	Elliptic Curves mod n	59
	Exercises	67
3	Torsion Points	73
3.1	Torsion Points	73
3.2	Division Polynomials	76
3.3	The Weil Pairing	82
	Exercises	86
4	Elliptic Curves over Finite Fields	89
4.1	Examples	89
4.2	The Frobenius Endomorphism	92
4.3	Determining the Group Order	96
4.3.1	Subfield Curves	96
4.3.2	Legendre Symbols	98
4.3.3	Orders of Points	100
4.3.4	Baby Step, Giant Step	103
4.4	A Family of Curves	105
4.5	Schoof's Algorithm	113

4.6	Supersingular Curves	120
	Exercises	130
5	The Discrete Logarithm Problem	133
5.1	The Index Calculus	134
5.2	General Attacks on Discrete Logs	136
5.2.1	Baby Step, Giant Step	136
5.2.2	Pollard's ρ and λ Methods	137
5.2.3	The Pohlig-Hellman Method	141
5.3	The MOV Attack	144
5.4	Anomalous Curves	147
5.5	The Tate-Lichtenbaum Pairing	153
5.6	Other Attacks	156
	Exercises	156
6	Elliptic Curve Cryptography	159
6.1	The Basic Setup	159
6.2	Diffie-Hellman Key Exchange	160
6.3	Massey-Omura Encryption	163
6.4	ElGamal Public Key Encryption	164
6.5	ElGamal Digital Signatures	165
6.6	The Digital Signature Algorithm	168
6.7	A Public Key Scheme Based on Factoring	169
6.8	A Cryptosystem Based on the Weil Pairing	173
	Exercises	175
7	Other Applications	179
7.1	Factoring Using Elliptic Curves	179
7.2	Primality Testing	184
	Exercises	187
8	Elliptic Curves over \mathbb{Q}	189
8.1	The Torsion Subgroup, The Lutz-Nagell Theorem	189
8.2	Descent and the Weak Mordell-Weil Theorem	198
8.3	Heights and the Mordell-Weil Theorem	206
8.4	Examples	214
8.5	The Height Pairing	221
8.6	Fermat's Infinite Descent	222
8.7	2-Selmer Groups; Shafarevich-Tate Groups	227
8.8	A Nontrivial Shafarevich-Tate Group	229
8.9	Galois Cohomology	234
	Exercises	244

9 Elliptic Curves over \mathbb{C}	247
9.1 Doubly Periodic Functions	247
9.2 Tori are Elliptic Curves	257
9.3 Elliptic Curves over \mathbb{C}	262
9.4 Computing Periods	275
9.4.1 The Arithmetic-Geometric Mean	277
9.5 Division Polynomials	283
Exercises	291
10 Complex Multiplication	295
10.1 Elliptic Curves over \mathbb{C}	295
10.2 Elliptic Curves over Finite Fields	302
10.3 Integrality of j -invariants	306
10.4 Numerical Examples	314
10.5 Kronecker's Jugendtraum	320
Exercises	321
11 Divisors	323
11.1 Definitions and Examples	323
11.2 The Weil Pairing	333
11.3 The Tate-Lichtenbaum Pairing	338
11.4 Computation of the Pairings	341
11.5 Genus One Curves and Elliptic Curves	346
Exercises	353
12 Zeta Functions	355
12.1 Elliptic Curves over Finite Fields	355
12.2 Elliptic Curves over \mathbb{Q}	359
Exercises	368
13 Fermat's Last Theorem	371
13.1 Overview	371
13.2 Galois Representations	374
13.3 Sketch of Ribet's Proof	380
13.4 Sketch of Wiles's Proof	387
A Number Theory	397
B Groups	403
C Fields	407
References	415
Index	425